| | | 1 | | | |
|------|---|----------------------------|-------------------------|----------------------------|-------------------------|
| | | | | | |
| | | | | | |
| Srno | Question | Option A | Option B | Option C | Option D |
| | | | Symmetric and | | |
| 1 | What are the two main types of cryptosystems? | Classical and Modern | Asymmetric | Public and Private | Static and Dynamic |
| | | Different keys are used | The encryption key is | The same key is used for | |
| | | for encryption and | public and decryption | both encryption and | |
| 2 | In a symmetric key encryption system | decryption | key is private | decryption | No key is required |
| | Which of the following is a component of a | | , , | | , , |
| 3 | cryptosystem? | Firewall | Encryption Algorithm | Web Server | Router |
| | The Caesar Cipher is a type of: | Transposition Cipher | Public Key Cipher | Substitution Cipher | Hashing Algorithm |
| _ | The Caesar Cipher is a type or. | Transposition cipilei | rublic key cipilei | Substitution cipilei | Trastiling Algorithm |
| _ | Vigenère Cipher is a type of: | Monoalphabetic Cipher | Polyalphabetic Cipher | Transposition Cipher | Block Cipher |
| | | Monoalphabetic Cipner | Polyaiphabetic cipilei | Transposition cipilei | Block cipilei |
| 6 | Which cipher rearranges the letters of the plaintext without changing the actual letters? | Caesar Cipher | Transposition Cipher | Monoalphabetic Cipher | Vigenère Cipher |
| 7 | DES is an example of: | <u>'</u> | | · | Hash Function |
| | How many keys are used in Triple DES? | Public Key Encryption | Stream Cipher 2 or 3 | Block Cipher | nash runction |
| - 0 | How many keys are used in Triple DES! | | | Applied Engraption | Advanced Electronic |
| | AFC storeds form | Automated Encryption | Advanced Encryption | Applied Encryption | |
| 9 | AES stands for: | Standard | Standard | Scheme | Security |
| 4.0 | A distribution of the second states | | 1.1 | Authentication and | E |
| - | A digital signature provides: | Confidentiality | Integrity | Integrity | Encryption |
| 11 | Which of the following ensures data integrity? | Encryption | Decryption | Hashing | Compression |
| | | | | Increased resource | It removes |
| 12 | One major drawback of cryptography is: | Reduced data accuracy | | consumption | authentication |
| | | A symmetric key | A type of hashing | A digital currency built | |
| | Bitcoin is: | algorithm | function | on blockchain | A digital signature |
| 14 | Blockchain stores data in: | Files | Tables | Blocks | Packets |
| | | Only one party holds the | | Data is stored at multiple | |
| 15 | A distributed ledger in blockchain means: | data | A centralized database | nodes | The ledger is printed |
| | Which of the following is not an attack on | | | | |
| 16 | cryptosystems? | Brute-force attack | Ciphertext-only attack | Firewall bypass | Known-plaintext attack |
| | | | | | |
| 17 | Asymmetric encryption is also known as: | Public key encryption | Symmetric encryption | Stream encryption | Substitution encryption |
| | | | | No need to share secret | |
| 18 | The main advantage of asymmetric encryption is: | Speed | Larger key size | keys | Simplicity |
| | | Different substitution for | A fixed substitution | A numeric | |
| 19 | Monoalphabetic cipher uses: | each letter | throughout | transformation | Bitwise operations |
| | Which cipher is considered the simplest form of | | | | |
| 20 | substitution cipher? | Vigenère Cipher | Caesar Cipher | Enigma Cipher | One-Time Pad |

| Srno | Question | Option A | Option B | Option C | Option D |
|------|--|------------------------|-------------------------|---|------------------------------|
| | Which traditional cipher is the most vulnerable to | | o position in | - Process | |
| 21 | frequency analysis? | Vigenère Cipher | Caesar Cipher | Transposition Cipher | Monoalphabetic Cipher |
| | Which key size is commonly used in AES? | 64-bit | 128-bit | 512-bit | 32-bit |
| | | | | Generate message | |
| 23 | Hash functions are primarily used to: | Encrypt messages | Sign digital documents | digests | Compress data |
| | Which one is not a modern symmetric encryption | | | | |
| 24 | algorithm? | AES | DES | RSA | Triple DES |
| 25 | In cryptography, a message digest refers to: | Compressed message | Encrypted file | Hash output | Decrypted data |
| | Which cryptographic tool helps verify that data has | | | | |
| 26 | not been altered? | Digital certificate | Encryption | Digital signature | Steganography |
| 27 | A benefit of cryptography in network security is: | Increasing bandwidth | Reducing latency | Ensuring confidentiality and authentication | Slowing down intruders |
| | | Their vulnerability to | Their dependence on | | Limited usage in modern |
| 28 | One drawback of strong cryptographic algorithms is: | physical attacks | outdated technology | High computational cost | systems |
| | | Converts plaintext to | Creates a fixed-length | | |
| 29 | A hash function in blockchain: | ciphertext | output from any input | Encrypts entire blocks | Verifies user identity |
| | The factor of the Philadelphia Challes and the state of the same | F | Controlly and an about | Hash chaining between | |
| 30 | The immutability of blockchain is due to: | Encrypted backups | Centralized control | blocks | Secure cloud storage |
| 24 | | Daamustian and | For any ordinal control | Both encryption and | Company time through welling |
| 31 | In asymmetric encryption, the public key is used for: | Decryption only | Encryption only | decryption | Generating hash values |
| 22 | The cocurity of asymmetric anymogystoms relies on | Drivata naturarka | Cogramy of algorithms | Computational difficulty of mathematical | Data compression |
| 32 | | Private networks | Secrecy of algorithms | problems | Data compression |
| 22 | Which attack uses precomputed hash values to crack passwords? | Brute-force attack | Dictionary attack | Rainbow table attack | Chasan plaintayt attack |
| 33 | | Brute-force attack | Dictionary attack | Railibow table attack | Chosen-plaintext attack |
| 34 | Which cipher was used by Julius Caesar in ancient times? | Monoalphabetic Cipher | Vigenère Cipher | Caesar Cipher | Transposition Cipher |
| 34 | Which cipher technique involves rearranging the | onoaiphabetic cipilei | Theries espiles | Cacoar cipilei | Transposition cipilei |
| 35 | order of characters? | Substitution | Transposition | Hybrid | Hashing |
| | What makes polyalphabetic ciphers stronger than | | Multiple substitution | , | , i |
| 36 | monoalphabetic ciphers? | Larger keys | alphabets | Use of XOR operations | Reverse encryption |
| 37 | RSA is based on the mathematical difficulty of: | Integer division | Prime factorization | Matrix inversion | Modular addition |

| Srno | Question | Option A | Option B | Option C | Option D |
|------|---|--------------------------|--------------------------|----------------------------|---|
| | The key length of RSA typically used for secure | | | | |
| 38 | communications is: | 56-bit | 128-bit | 2048-bit | 64-bit |
| | Which of the following is not a property of a good | | | | |
| 39 | hash function? | Deterministic output | Reversibility | Collision resistance | Fixed-length output |
| | | | | | |
| | | The same input gives | Two different inputs | The hash function fails to | |
| 40 | A collision in a hash function means: | different outputs | produce the same hash | run | The key is exposed |
| | | | | Provides data | |
| | Which of the following is an advantage of | Eliminates need for | | confidentiality and | |
| 41 | cryptography? | passwords | Increases network speed | integrity | Allows easy key sharing |
| 42 | Cryptography does not protect against: | Data tampering | Network sniffing | User impersonation | Physical theft of data |
| | | | Timestamp and hash of | | |
| 43 | Each block in a blockchain contains: | Only transaction data | the previous block | Public key and signature | A single user's data |
| | | | | | |
| 44 | Blockchain uses consensus algorithms to: | Encrypt data | Verify transactions | Store private keys | Decode hash functions |
| | Which of the following is a key feature of blockchain | | | | |
| 45 | technology? | Centralized ledger | Immutable records | Hidden transactions | Open file sharing |
| | | | | | |
| | | | A structure that defines | | |
| | | A program used to send | encryption, decryption, | A system for digital | A public ledger of |
| 46 | Which of the following best defines a cryptosystem? | messages | and key management | marketing | transactions |
| | | | Only used to encrypt | Kept secret and used to | Used to generate hash |
| 47 | In public-key cryptography, the private key is: | Shared with everyone | messages | decrypt messages | values |
| | | , | _ | | |
| | | | | Choose arbitrary | |
| | Chosen-plaintext attack (CPA) means the attacker | | | plaintexts to encrypt and | Modify the encryption |
| 48 | can: | Only see the ciphertext | Only see the public key | observe ciphertexts | algorithm |
| | | , | Limited number of | Complexity of the | - |
| 49 | The weakness of Caesar cipher is due to: | Its use of a private key | possible shifts (25) | algorithm | One-time pads |
| | ' | , , , , | . , | | ' |
| | | Shifts letters based on | | Replaces each character | |
| 50 | What does a substitution cipher do? | their position | Rearranges characters | with another | Encrypts using a key pair |
| | ' | ' | | | ,, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, |
| | Which cipher is considered unbreakable if used | | | | |
| 51 | · | Caesar Cipher | Vigenère Cipher | One-Time Pad | Transposition Cipher |
| | , , , , | ' | ' | | ' ' |

| Srno | Question | Option A | Option B | Option C | Option D |
|------|---|--------------------------|---------------------------|---------------------------|---------------------------|
| | Which modern algorithm is most widely used in | | | | |
| | securing wireless networks (e.g., WPA2)? | DES | RSA | AES | MD5 |
| 53 | The output of a hash function is called: | Key | Message digest | Signature | Ciphertext |
| | Which algorithm is considered insecure today due to | | | | |
| | its small key size and vulnerability to brute-force | | | | |
| 54 | attacks? | AES | SHA-256 | DES | RSA-2048 |
| | Which term describes the ability to detect | | | | |
| 55 | unauthorized changes to data? | Confidentiality | Authenticity | Integrity | Obfuscation |
| | | | | | |
| 56 | A digital signature is typically created using: | Hashing only | Symmetric encryption | A sender's private key | A recipient's public key |
| | | | It cannot be used over | It is slower than | It uses the same key for |
| 57 | One limitation of public key encryption is: | It is not secure | the internet | symmetric encryption | both parties |
| | | | | | |
| | Which of the following consensus mechanisms is | | Delegated Proof of Stake | | Practical Byzantine Fault |
| 58 | used in Bitcoin? | Proof of Stake (PoS) | (DPoS) | Proof of Work (PoW) | Tolerance (PBFT) |
| | The process of verifying and adding transactions to | | | | |
| 59 | the blockchain is known as: | Mining | Forking | Hashing | Signing |
| | | | Only administrators can | Once written, data | Data is encrypted with |
| 60 | In blockchain, immutability means: | The chain is centralized | modify data | cannot be changed | private keys |
| | Which property ensures that only the intended | | | | |
| 61 | recipient can read a message? | Integrity | Confidentiality | Availability | Authentication |
| | Which cryptographic method uses two keys | | | | |
| 62 | mathematically linked together? | Caesar Cipher | Stream Cipher | Public Key Cryptography | Hashing |
| | | | | | |
| | | | | Generating, distributing, | |
| | What is key management in cryptography concerned | Designing cipher | | and storing | |
| 63 | with? | algorithms | Creating long passwords | cryptographic keys | Encrypting images |
| | Which cipher type is most affected by letter | | | | |
| 64 | frequency analysis? | Caesar Cipher | Vigenère Cipher | Transposition Cipher | One-Time Pad |
| | | | | Applying multiple Caesar | |
| | The Vigenère cipher combats letter frequency | Using mathematical | | shifts based on a | |
| 65 | attacks by: | operations | Shifting letters randomly | keyword | Scrambling bits |
| | | | | | |
| 66 | A transposition cipher maintains: | The order of letters | The letter frequency | The position of the key | None of the above |
| | Which algorithm is commonly used for digital | | | | |
| 67 | certificates? | AES | DES | RSA | Blowfish |
| | | | | | |

| Srno | Question | Option A | Option B | Option C | Option D |
|------|--|-------------------------|----------------------------|---------------------------|---------------------------|
| | | • | | | · |
| 68 | Which of the following is a secure hash function? | MD4 | MD5 | SHA-256 | SHA-1 |
| | | | | | |
| 69 | In a digital signature, the verification is done using: | Sender's public key | Receiver's private key | Receiver's public key | Sender's private key |
| | | | | Unauthorized access and | |
| 70 | Cryptography helps prevent: | Email spam | Data loss | tampering | Operating system failure |
| 71 | Which of the following is not a goal of cryptography? | Confidentiality | Data redundancy | Integrity | Non-repudiation |
| | The state of the second | - Community | | | |
| | | The message cannot be | The sender cannot deny | The message cannot be | The recipient cannot |
| 72 | Non-repudiation ensures: | intercepted | sending the message | altered | view the message |
| | What does the blockchain term "genesis block" refer | The latest block in the | | The first block in the | |
| 73 | to? | chain | A hash function | blockchain | A mining algorithm |
| | | | Public access to the | | |
| 74 | What ensures transparency in blockchain systems? | Hidden records | ledger | Password encryption | Restricted consensus |
| | Which of the following makes blockchain resistant to | | | Cryptographic hash | |
| 75 | tampering? | Centralized servers | Frequent updates | linking of blocks | Open-source licensing |
| | Which of the following algorithms is not used for | | | | |
| | encryption? | AES | SHA-256 | DES | RSA |
| | The effectiveness of brute-force attacks can be | | | | |
| // | reduced by: | Shorter keys | Hashing the ciphertext | Using strong, longer keys | Sending plaintext instead |
| | | | Slow down attackers by | Convert passwords to | |
| 78 | The purpose of salting in password storage is to: | Encrypt the passwords | adding randomness | base64 | Make hashing reversible |
| | The parpose of salaing in passivora storage is to | Zitorype are passivorus | A private key to a hash | A public key to an | A message to a time |
| 79 | A digital certificate binds: | A user to an IP address | function | identity | stamp |
| | | | | , | ' |
| | | | | A combination of | |
| | | Only symmetric | | symmetric and | |
| 80 | SSL/TLS protocols use: | encryption | Only hashing | asymmetric encryption | Steganography |
| 81 | A strong hash function must be resistant to: | Compression | Random inputs | Collisions | Encryption |
| | | | | | |
| | | Encrypt the entire | Ensure message | | |
| 82 | | message | authenticity and integrity | Store private keys | Hash passwords |
| | Which algorithm uses block ciphers in rounds and | | | | |
| 83 | substitution-permutation networks? | DES | RSA | Vigenère Cipher | SHA-1 |

| 84 How many rounds does AE5-128 perform? 85 What is the block size of DE5 is: 86 The block size of DE5 is: 87 Which attack assumes access to both plaintext and ciphertext? 88 The Avalanche Effect in cryptography means: 89 Which key pair is used in digital signatures? 90 What is blockchain mining? 91 Which type of encryption is faster in execution? 92 In cryptography, non-repudilation ensures: Which cryptographic technique is widely used in 93 blockchain for linking blocks? 93 Which exercised and in the process of making encrypted data readable 95 again is called: 94 The SHA-256 algorithm always outputs a hash of: The process of making encrypted data readable 95 again is called: 95 Which of these is true about the Caesar cipher? 96 Which of these is true about the Caesar cipher? 97 Which of these is true about the Caesar cipher? 98 Which of the Following is a symmetric encryption 99 algorithm? 99 Which of the following is a symmetric encryption 99 algorithm? 90 Which of the following is a symmetric encryption 99 algorithm? 90 Which of the following is a symmetric encryption 99 algorithm? 91 Which of the following is a symmetric encryption 99 algorithm? 92 Which define the following is a symmetric encryption 99 algorithm? 93 Which attack assumes access to both plaintext attack of this is a polyalphabetic cipher or profer attack of the following is a symmetric encryption 99 attack of the following is a symmetric encryption 99 algorithm? 94 Which of the following is a symmetric encryption 99 algorithm? 95 Which of the following is a symmetric encryption 99 algorithm? 96 Which of the following is a symmetric encryption 99 algorithm? 97 Which attack is based on measuring physical 100 information like timing and power usage? 98 Brute-force attack 50 is bits 128 bits 100 information like timing and power usage? 99 Brute-force attack 50 is 64 bits 120 is 64 bi | | | | | | |
|--|-----|---|---------------------------|---------------------------------------|---|---------------------------|
| 85 What is the block size of AES? 86 The block size of DES is: 128 bits 86 bits 95 bits 92 bits 93 bits 94 bits 95 bits 95 bits 92 bits 95 bits 92 bits 95 bits 96 bits 97 bits 98 bits 98 bits 98 bits 99 Which key pair is used in digital signatures? 90 What is blockchain mining? 91 Which type of encryption is faster in execution? 92 In cryptography, non-repudiation ensures: 93 blockchain for linking blocks? 94 The SHA-256 algorithm always outputs a hash of: 176 bits 176 bits 178 bits 188 bits 189 bits 189 bits 180 bits 1 | | • | • | • | • | |
| Which attack assumes access to both plaintext and 87 ciphertext? Ciphertext-only attack Chosen-plaintext attack Small input change Causes major output Causes major | | | | | | 16 |
| Which attack assumes access to both plaintext and 27 ciphertext? Which attack assumes access to both plaintext and 37 ciphertext? All keys generate similar causes major output ciphertext change acauses major output for previde acauses | - | | | | | |
| 87 ciphertext? Ciphertext-only attack All keys generate similar clauses major output change All keys generate similar ciphertext All keys generate similar clauses major output change Private key to sign, public key to sign, public key to sign, public key to verify private key to verify private key to verify for verification What is blockchain mining? Buying cryptocurrency Asymmetric Asymmetric Public-key Symmetric Digital signature Which tryptography, non-repudiation ensures: Which cryptography, non-repudiation ensures: Which cryptography, non-repudiation ensures: Which cryptographic technique is widely used in 30 blockchain for linking blocks? Yigenère Cipher Hashing RSA AES Which of these is true about the Caesar cipher? It uses random keys algain is called: Triple DES performs how many DES operations? Which attack is based on measuring physical look in for linking blower usage? Which attack is based on measuring physical look in for linking blower usage? Brute-force attack Small input change All keys generate similar caucauses major output change The algorithm is unstable crash. Small input change The algorithm is unstable crash. Small input change The algorithm is unstable crash. Both private key to verify private keys to verify priva | 86 | | 128 bits | 64 bits | 56 bits | 32 bits |
| All keys generate similar ciphertext cipher private key to sign, public key to sign, private key to verify Verifying transactions and adding them to the chain did to the chain | 87 | · | Ciphertext-only attack | Chosen-plaintext attack | Known-plaintext attack | Side-channel attack |
| All keys generate similar ciphertext ciphertext change The algorithm is unstable crash The Avalanche Effect in cryptography means: All keys generate similar ciphertext change The algorithm is unstable crash Private key to sign, public key to verify private key to verify for verification Symmetric keys Verifying transactions and adding them to the chain Buying cryptocurrency networks Public-key Symmetric Digital signature Public-key Symmetric Digital signature Public-key Symmetric Digital signature The message has not been altered having sent the message confidential The system can be resulted again is called: The process of making encrypted data readable again is called: Which of these is true about the Caesar cipher? Which of these is true about the Caesar cipher? Which of the following is a symmetric encryption Passage Asson to be altered having sent the message confidential The system can be resulted to the special again is called: Transposition Hashing Decryption Variable length Too complex for practical use Small key size (56 bits) Which of the following is a symmetric encryption Passage Asson to be altered having sent the message remains confidential The system can be resulted to the sent true about the Caesar cipher? It uses random keys to specify the specific again is called: Transposition Hashing Decryption Obfuscation It is a polyalphabetic cipher and without substitution Vulnerable to chosen-plaintext attacks only Passage Asson to be altered having sent the message remains confidential The system can be resulted to the sent true about the Caesar cipher? It uses random keys to specify the specific again is called: Too complex for practical use Small key size (56 bits) Which attack is based on measuring physical only information like timing and power usage? Provide key to verify private key to verify private and public cipher the dading them to the chain adding them to the cha | | 1 | , | · · | ' | |
| 88 The Avalanche Effect in cryptography means: 89 Which key pair is used in digital signatures? 90 What is blockchain mining? 91 Which type of encryption is faster in execution? 92 In cryptography, non-repudiation ensures: 93 Which cryptography, non-repudiation ensures: 94 The SHA-256 algorithm always outputs a hash of: The process of making encrypted data readable 95 again is called: 96 Which of these is true about the Caesar cipher? 97 The main weakness of DES today is: 98 Which of the following is a symmetric encryption 99 B Triple DES performs how many DES operations? 99 Which of the following is a symmetric encryption algorithm? 90 What is blockchain mining? 91 Which key pair is used in digital signatures? 92 In cryptographic technique is widely used in 93 blockchain for linking blocks? 94 The SHA-256 algorithm always outputs a hash of: 128 bits 129 bits a polyalphabetic cipher 129 Which of these is true about the Caesar cipher? 120 The main weakness of DES today is: 95 Triple DES performs how many DES operations? 96 Which of the following is a symmetric encryption algorithm? 97 The main measuring physical information like timing and power usage? 98 Brute-force attack 99 Standard they to verify private key to verify provide key to verify private key to verify private key to verify provide they to verify for verification Symmetric head adding them to the chain 80 Both private key to verify private and public for verification Symmetric encryption and adding them to the chain 129 The message has not public-key 120 Symmetric 121 Symmetric 122 Symmetric 123 Symmetric 123 Symmetric 124 Symmetric 125 Sits 126 Sits 127 Sits and public for verification 128 Decryptocurrency 129 Sits and adding them to the chain 129 Sits and adding them to the chain 129 Sy | | | All keys generate similar | | | The encryption causes a |
| Private key to sign, public key to sign, public key to sign, public key to verify private key to verify private key to verify for verification Symmetric keys Verifying transactions and adding them to the chain networks 91 Which type of encryption is faster in execution? Asymmetric Public-key Public-key Symmetric Public-key Symmetric Digital signature The message has not been altered having sent the message remains confidential The system can be resulted to find the system can be resulted to f | 88 | The Avalanche Effect in cryptography means: | , - | · · · | The algorithm is unstable | |
| Symmetric keys Public key to verify Private key | | The Availation of Energy and Property means: | - | _ | | 0.0311 |
| Verifying transactions and adding them to the chain Buying cryptocurrency heacking into blockchain mining? 91 Which type of encryption is faster in execution? Asymmetric Public-key Symmetric Digital signature The message has not been altered having sent the message remains confidential The system can be resulted. Which cryptographic technique is widely used in 93 blockchain for linking blocks? 94 The SHA-256 algorithm always outputs a hash of: 128 bits 64 bits 256 bits Variable length The process of making encrypted data readable sagain is called: Transposition Hashing Decryption Obfuscation It is a polyalphabetic cipher number without substitution 150 complex for practical use Small key size (56 bits) Plaintext attacks only 98 Triple DES performs how many DES operations? 1 2 3 Which of the following is a symmetric encryption 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical 100 information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attacks Cipheration It attacks Side-channel attack Known-plaintext attacks Cipheratical Ciphertext-only attacled. | 89 | Which key nair is used in digital signatures? | | | | Symmetric keys |
| and adding them to the chain Buying cryptocurrency networks 91 Which type of encryption is faster in execution? Asymmetric Public-key Symmetric Digital signature The message has not been altered baving sent the message confidential The system can be restricted by this process of making encrypted data readable pagain is called: Transposition Transposition Hashing Decryption Diffusion of these is true about the Caesar cipher? It uses random keys Pagarinis without substitution Profession of the following is a symmetric encryption and adding them to the chain declaration blockchain metworks Asymmetric Public-key Symmetric Digital signature The message remains having sent the message confidential The system can be restricted by the saving sent the message of the sender cannot deny having sent the message remains confidential The system can be restricted. The process of making blockchain for linking blocks? 94 The SHA-256 algorithm always outputs a hash of: The process of making encrypted data readable pagain is called: Transposition Hashing Decryption Diffuscation It say a polyalphabetic cipher It uses random keys cipher number without substitution Vulnerable to chosen-proof Practical use Small key size (56 bits) Proof Small key size (56 bits) Proof Small key size (56 bits) Proof Small key size (56 bits) DSA Which of the following is a symmetric encryption algorithm? Which attack is based on measuring physical information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | 03 | Willest Key pair is asea in digital signatures: | public key to verify | · · · · · · · · · · · · · · · · · · · | Tor vermeation | Symmetric Reys |
| 90 What is blockchain mining? Encrypting wallets chain Buying cryptocurrency networks 91 Which type of encryption is faster in execution? Asymmetric Public-key Symmetric Digital signature The message has not been altered having sent the message confidential The system can be resembled. Which cryptography, non-repudiation ensures: Which cryptography, non-repudiation ensures: Which cryptographic technique is widely used in 93 blockchain for linking blocks? Vigenère Cipher Hashing RSA AES 94 The SHA-256 algorithm always outputs a hash of: 128 bits 64 bits 256 bits Variable length The process of making encrypted data readable again is called: Transposition Hashing Decryption Obfuscation It is a polyalphabetic cipher unumber without substitution Vigenère Cipher Hashing Decryption Obfuscation It is a polyalphabetic cipher on number Without substitution Vulnerable letters without substitution 1 to complex for practical use Small key size (56 bits) Partiple DES performs how many DES operations? Which of the following is a symmetric encryption 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attacle | | | | | | Hacking into blockchain |
| 91 Which type of encryption is faster in execution? Asymmetric The message has not been altered Which cryptography, non-repudiation ensures: Which cryptographic technique is widely used in 93 blockchain for linking blocks? Vigenère Cipher Hashing RSA AES 4 The SHA-256 algorithm always outputs a hash of: The process of making encrypted data readable again is called: Which of these is true about the Caesar cipher? It uses random keys Lack of mathematical proof Public-key Symmetric Digital signature Digital signature The sender cannot deny having sent the message confidential The system can be resulted to the system can be resulted having sent the message remains having sent the message confidential The system can be resulted to the system can be resulted having sent the message remains having sent the | 00 | What is blockshain mining? | Encrypting wallots | _ | Puving cryptocurrency | _ |
| The message has not been altered having sent the message remains confidential The system can be resulted having sent the message remains confidential The system can be resulted having sent the message remains confidential The system can be resulted having sent the message remains confidential The system can be resulted for inking blocks? 94 The SHA-256 algorithm always outputs a hash of: 128 bits 64 bits 256 bits Variable length Transposition Hashing Decryption Obfuscation It is a polyalphabetic cipher unmber without substitution It is a polyalphabetic cipher number Which of these is true about the Caesar cipher? Lack of mathematical proof The main weakness of DES today is: Transposition AES Variable length Transposition It is a polyalphabetic cipher number without substitution Vulnerable to chosen-proof Practical use Small key size (56 bits) Which of the following is a symmetric encryption 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | 90 | Wildt is blockcridin minning: | Eliciypting wallets | Citalii | buying cryptocurrency | HELWOIKS |
| 92 In cryptography, non-repudiation ensures: Which cryptographic technique is widely used in blockchain for linking blocks? 94 The SHA-256 algorithm always outputs a hash of: The process of making encrypted data readable again is called: 95 Which of these is true about the Caesar cipher? Which of these is true about the Caesar cipher? It uses random keys cipher Which of these is true about the Caesar cipher? It uses random keys cipher It uses random keys cipher Too complex for practical use Partiple DES performs how many DES operations? Which of the following is a symmetric encryption 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | 91 | Which type of encryption is faster in execution? | Asymmetric | Public-key | Symmetric | Digital signature |
| 92 In cryptography, non-repudiation ensures: Which cryptographic technique is widely used in blockchain for linking blocks? Vigenère Cipher Hashing RSA AES 94 The SHA-256 algorithm always outputs a hash of: The process of making encrypted data readable again is called: Which of these is true about the Caesar cipher? It uses random keys Which of these is true about the Caesar cipher? It uses random keys Lack of mathematical proof Proof The main weakness of DES today is: The process of making encrypted data readable 95 Which of these is true about the Caesar cipher? It uses random keys Lack of mathematical proof Proof Which of the following is a symmetric encryption 98 Triple DES performs how many DES operations? Which of the following is a symmetric encryption 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | | | | | | |
| 92 In cryptography, non-repudiation ensures: Which cryptographic technique is widely used in blockchain for linking blocks? 94 The SHA-256 algorithm always outputs a hash of: The process of making encrypted data readable again is called: 95 Which of these is true about the Caesar cipher? Which of these is true about the Caesar cipher? It uses random keys cipher Which of these is true about the Caesar cipher? It uses random keys cipher It uses random keys cipher Too complex for practical use Partiple DES performs how many DES operations? Which of the following is a symmetric encryption 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | | | The message has not | The sender cannot deny | The message remains | |
| Which cryptographic technique is widely used in blockchain for linking blocks? Vigenère Cipher Hashing RSA AES 4ES 4ES 4ES 4ES 4ES 4ES | 92 | In cryptography, non-repudiation ensures: | <u> </u> | having sent the message | _ | The system can be reset |
| 93 blockchain for linking blocks? Vigenère Cipher Hashing RSA AES 94 The SHA-256 algorithm always outputs a hash of: The process of making encrypted data readable again is called: Transposition Hashing Decryption Obfuscation It is a polyalphabetic cipher Without substitution Lack of mathematical proof Transposition It uses random keys Lack of mathematical proof Too complex for practical use Small key size (56 bits) Which of the following is a symmetric encryption 98 Triple DES performs how many DES operations? Which of the following is a symmetric encryption 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | | | | <u> </u> | | , |
| 94 The SHA-256 algorithm always outputs a hash of: The process of making encrypted data readable 95 again is called: Transposition Hashing Decryption Obfuscation It is a polyalphabetic cipher Number Without substitution Lack of mathematical proof Too complex for practical use Practical use Triple DES performs how many DES operations? Triple DES performs how many DES operations? Which of the following is a symmetric encryption 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical 100 information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | 93 | | Vigenère Cipher | Hashing | IRSA | AES |
| The process of making encrypted data readable 95 again is called: Transposition Hashing Decryption Obfuscation It is a polyalphabetic cipher number Without substitution Too complex for practical use 96 Which of these is true about the Caesar cipher? The main weakness of DES today is: Triple DES performs how many DES operations? Which of the following is a symmetric encryption 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical 100 information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | | <u> </u> | | Ü | | |
| The process of making encrypted data readable 95 again is called: Transposition Hashing Decryption Obfuscation It is a polyalphabetic cipher number Without substitution Too complex for practical use 96 Which of these is true about the Caesar cipher? The main weakness of DES today is: Triple DES performs how many DES operations? Which of the following is a symmetric encryption 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical 100 information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | 94 | The SHA-256 algorithm always outputs a hash of: | 128 bits | 64 bits | 256 bits | Variable length |
| 95 again is called: Transposition Hashing Decryption Obfuscation It is a polyalphabetic cipher number Without substitution Lack of mathematical proof Triple DES performs how many DES operations? Which of the following is a symmetric encryption 99 algorithm? RSA Which attack is based on measuring physical 100 information like timing and power usage? Transposition Hashing Decryption Obfuscation It is a polyalphabetic cipher number No complex for practical use Small key size (56 bits) Vulnerable to chosen-plaintext attacks only Vulnerable to chosen-plaintext attacks only AES DSA Which attack is based on measuring physical 100 information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | | | | | | |
| 96 Which of these is true about the Caesar cipher? It uses random keys cipher number without substitution Lack of mathematical proof The main weakness of DES today is: Too complex for practical use Small key size (56 bits) Which of the following is a symmetric encryption 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical 100 information like timing and power usage? Brute-force attack It is a polyalphabetic cipher number Number Number Number Vulnerable to chosen-practical use Small key size (56 bits) Small key size (56 bits) Vulnerable to chosen-practical use Small key size (56 bits) Side-channel attack Known-plaintext attack Ciphertext-only attack | 95 | | Transposition | Hashing | Decryption | Obfuscation |
| 96 Which of these is true about the Caesar cipher? It uses random keys Lack of mathematical proof The main weakness of DES today is: 97 The main weakness of DES today is: 98 Triple DES performs how many DES operations? Which of the following is a symmetric encryption 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | | wanni o cancar | Тапоросного | - | , , , | |
| Description Lack of mathematical Too complex for practical use Small key size (56 bits) Plaintext attacks only 98 Triple DES performs how many DES operations? 1 2 3 Which of the following is a symmetric encryption 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical 100 information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack Ciph | 96 | Which of these is true about the Caesar cipher? | It uses random keys | | · · | |
| 97 The main weakness of DES today is: proof practical use Small key size (56 bits) plaintext attacks only 98 Triple DES performs how many DES operations? Which of the following is a symmetric encryption 99 algorithm? RSA Which attack is based on measuring physical 100 information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | 30 | Trinon of these is true about the edesar eighter. | | • | - Individual of the second of | |
| 98 Triple DES performs how many DES operations? Which of the following is a symmetric encryption 99 algorithm? RSA Which attack is based on measuring physical 100 information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | 97 | The main weakness of DFS today is: | | ' | Small key size (56 hits) | |
| Which of the following is a symmetric encryption 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical 100 information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | | The main weakiness of BES today is. | P. 001 | practical asc | 3.1.dii Key 3120 (30 bit3) | plantecke accacks offing |
| 99 algorithm? RSA SHA-1 AES DSA Which attack is based on measuring physical 100 information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | 98 | Triple DES performs how many DES operations? | 1 | 2 | 3 | 6 |
| Which attack is based on measuring physical 100 information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | | Which of the following is a symmetric encryption | | | | |
| 100 information like timing and power usage? Brute-force attack Side-channel attack Known-plaintext attack Ciphertext-only attack | 99 | algorithm? | RSA | SHA-1 | AES | DSA |
| | | Which attack is based on measuring physical | | | | |
| It is managed by a No single entity controls | 100 | information like timing and power usage? | Brute-force attack | Side-channel attack | Known-plaintext attack | Ciphertext-only attack |
| The international property of the property of | | | It is managed by a | No single entity controls | | |
| 101 Blockchain is considered decentralized because: central database the data It uses encryption only It works offline | 101 | Blockchain is considered decentralized because: | | | It uses encryption only | It works offline |

| Srno | Question | Option A | Option B | Option C | Option D |
|------|--|--------------------------|-----------------------|-------------------------|------------------------|
| | | | | | |
| 102 | A major benefit of public blockchains is: | High speed | Controlled access | Transparency and trust | Private user data |
| | | | | Chained hashes of | Frequent software |
| 103 | What ensures immutability in blockchain? | Centralized data servers | Editing capabilities | previous blocks | updates |
| | · | | | | |
| 104 | In asymmetric encryption, what is kept secret? | Public key | Decrypted data | Private key | Ciphertext |
| | , , , , , , | , | / / | , | <u>'</u> |
| 105 | Which one of the following is not a block cipher? | DES | AES | RSA | Blowfish |
| | дене по | | | | |
| | What is the primary function of a cryptographic hash | | | Generate a fixed-length | Create a digital |
| 106 | function? | Encrypt data | Compress data | output from input data | certificate |
| 100 | Which cryptographic concept ensures data has not | Literype data | compress data | output nom input data | certificate |
| 107 | been altered in transit? | Confidentiality | Integrity | Availability | Non-repudiation |
| 107 | Which of the following uses both substitution and | Connactitianty | Integrity | Availability | Non repudiation |
| 108 | transposition techniques? | Caesar cipher | Stream cipher | AES | One-time pad |
| | In asymmetric encryption, the sender uses: | Their own private key | Receiver's public key | Receiver's private key | Hash function |
| 109 | in asymmetric encryption, the sender uses. | Their own private key | Receiver 5 public key | Receiver 5 private key | nasii iulictioii |
| 110 | Which of those is considered a bashing algorithm? | RSA | SHA-256 | AES | ECC |
| 110 | Which of these is considered a hashing algorithm? | KSA | SHA-230 | AES | ECC |
| | | | Karria a atha a a d | | |
| | | | Key length and | | |
| 144 | The above the forest and the control of the control | The use of one secret | complexity of | | |
| 111 | The strength of asymmetric encryption lies in: | key | mathematical problems | Quick computation | Compression algorithms |
| | What is the most common key length used in RSA | | | | |
| 112 | today for secure communication? | 128 bits | 256 bits | 512 bits | 2048 bits |
| | | | A key management | A one-time random | |
| 113 | What is a cryptographic nonce? | A hash algorithm | protocol | number | A public key |
| | | | | | |
| 114 | Which cipher is polyalphabetic in nature? | Caesar Cipher | Monoalphabetic Cipher | Vigenère Cipher | Transposition Cipher |
| | Which of the following is a disadvantage of | | Needs a secure key | Only used for digital | |
| 115 | symmetric key encryption? | Too slow | exchange mechanism | signatures | Keys are public |
| | | | | Validate and record | Generate digital |
| 116 | What role do miners play in a blockchain? | Create new private keys | Reverse transactions | transactions | signatures for users |
| | | | | | |
| 117 | Which is not a feature of blockchain technology? | Decentralization | Transparency | Mutability | Security |
| | Which part of a blockchain block contains the hash | | | | |
| 118 | of the previous block? | Data | Timestamp | Nonce | Block header |
| | • | | • | • | • |

| Srno Question Option A Option B Option C Option D A cryptographic algorithm transactions A type of si What is the main purpose of blockchain consensus algorithms? Which of the following provides both integrity and authentication? Encryption Digital Signatures Caesar Cipher Hashing Uses complex Which one is a weakness of symmetric encryption? Myhich of these is a stream cipher? DES AES RC4 RSA 125 The key length of AES-256 is: Dictionary attack Unbreakable if used correctly Whashed Message with Hashed Message Whybrid Message Hidden MA Option B Option C Option D Option D Option D A cryptographic algorithm A record of all transactions A record of all transactions A type of si Ensure agreement on Improve network speed transaction validity Track walle Ensure agreement on Digital Signatures Caesar Cipher Hashing Uses complex Public key is hard to secure key distribution is required encryption Secure key distribution is Slower tha required encryption Secure key distribution is Slower tha required encryption AES RC4 RSA 125 The key length of AES-256 is: Dictionary attack Chosen-ciphertext attack Chosen | essage |
|--|-----------------------------|
| A cryptographic algorithm A record of all transactions A type of signatures? What is the main purpose of blockchain consensus algorithms? Which of the following provides both integrity and authentication? Encrypt data on the chain authentication? Encryption Digital Signatures Caesar Cipher Hashing What is a public key used for in digital signatures? Encrypt the message Generate a nonce Verify the signature Hash the mathematics store required encryption and the chain says the signature of | t addresses essage |
| A cryptographic algorithm A record of all transactions A type of si algorithms? What is the main purpose of blockchain consensus algorithms? Which of the following provides both integrity and 121 authentication? Encrypt data on the chain authentication? Encrypt on Digital Signatures Generate a nonce Verify the signature Hash the main purpose of blockchain consensus algorithms? Encrypt data on the chain authentication? Encrypt data on the chain algorithm blockchain consensus algorithms? Encrypt data on the chain algorithm blockchain consensus algorithms Encrypt data on the chain algorithm blockchain consensus algorithms Encrypt data on the chain algorithms E | t addresses essage |
| 119 The term 'ledger' in blockchain refers to: What is the main purpose of blockchain consensus 120 algorithms? Which of the following provides both integrity and 121 authentication? Encrypt the message What is a public key used for in digital signatures? Encrypt the message Uses complex mathematics 123 Which one is a weakness of symmetric encryption? 124 Which of these is a stream cipher? DES AES RC4 RSA 125 The key length of AES-256 is: Dictionary attack Unbreakable if used Unbreakable if used Correctly A mining device algorithm transactions A type of signature Encrypt data on the Improve network speed Interpreted Ensure agreement on transaction validity Track walle Ensure agreement on transaction va | t addresses essage |
| What is the main purpose of blockchain consensus 120 algorithms? Which of the following provides both integrity and 121 authentication? Encryption Digital Signatures Caesar Cipher Hashing What is a public key used for in digital signatures? Encrypt the message Uses complex mathematics Public key is hard to store Public key is hard to store required encryption 122 Which one is a weakness of symmetric encryption? DES AES RC4 RSA 125 The key length of AES-256 is: Dictionary attack Unbreakable if used correctly Caesar Cipher Hashing Hash the mathematics Slower tha required encryption Chosen-ciphertext attack Symmetric and deterministic Obsolete a | t addresses essage |
| 120 algorithms? Chain Improve network speed transaction validity Track waller Which of the following provides both integrity and 121 authentication? Encryption Digital Signatures Caesar Cipher Hashing 122 What is a public key used for in digital signatures? Encrypt the message Generate a nonce Verify the signature Hash the mathematics Secure key distribution is Slower that 123 Which one is a weakness of symmetric encryption? DES AES RC4 RSA 125 The key length of AES-256 is: 128 bits 192 bits 256 bits 512 bits 126 Which attack method tries every possible key? Dictionary attack Unbreakable if used Chosen-ciphertext attack Chos | essage |
| Which of the following provides both integrity and authentication? Encryption Digital Signatures Caesar Cipher Hashing Loses complex Public key is hard to store required Public key distribution is store Which one is a weakness of symmetric encryption? DES AES RC4 RSA 125 The key length of AES-256 is: Dictionary attack Which attack method tries every possible key? Dictionary attack Uses complex Public key is hard to secure key distribution is store required encryption AES RC4 RSA Solver that encryption DES AES RC4 RSA Solver that encryption AES RC4 RSA Tobe key length of AES-256 is: Dictionary attack Unbreakable if used correctly Chosen-ciphertext attack An example of block cipher deterministic Obsolete a | essage |
| 121 authentication? Encryption Digital Signatures Caesar Cipher Hashing 122 What is a public key used for in digital signatures? Encrypt the message Generate a nonce Verify the signature Hash the massage Uses complex mathematics public key is hard to secure key distribution is required encryption 123 Which one is a weakness of symmetric encryption? DES AES RC4 RSA 125 The key length of AES-256 is: 128 bits 129 bits 256 bits 512 bits 126 Which attack method tries every possible key? Unbreakable if used correctly Chosen-ciphertext attack An example of block Symmetric and deterministic Obsolete a | _ |
| 122 What is a public key used for in digital signatures? Encrypt the message Generate a nonce Verify the signature Hash the multiple of the signature Public key is hard to store required encryption encryption DES AES RC4 RSA 125 The key length of AES-256 is: 128 bits 192 bits 256 bits 512 bits 126 Which attack method tries every possible key? Dictionary attack Unbreakable if used 127 The one-time pad cipher is: Chosen-cipher deterministic Obsolete a correctly cipher | |
| Uses complex public key is hard to secure key distribution is slower that store required encryption? 124 Which of these is a stream cipher? 125 The key length of AES-256 is: 126 Which attack method tries every possible key? Dictionary attack Unbreakable if used correctly Chosen-ciphertext attack An example of block Symmetric and correctly Chosen-cipher deterministic Obsolete a | _ |
| Uses complex public key is hard to secure key distribution is slower that store required encryption? 124 Which of these is a stream cipher? 125 The key length of AES-256 is: 126 Which attack method tries every possible key? Dictionary attack Unbreakable if used correctly Chosen-ciphertext attack An example of block Symmetric and correctly Chosen-cipher deterministic Obsolete a | |
| 123 Which one is a weakness of symmetric encryption? mathematics store required encryption 124 Which of these is a stream cipher? DES AES RC4 RSA 125 The key length of AES-256 is: 128 bits 192 bits 256 bits 512 bits 126 Which attack method tries every possible key? Dictionary attack Chosen-ciphertext attack Brute-force attack Known-key 127 The one-time pad cipher is: Chosen-ciphertext attack Chosen-ciphertext Chosen- | asymmetric |
| 123 Which one is a weakness of symmetric encryption? mathematics store required encryption 124 Which of these is a stream cipher? DES AES RC4 RSA 125 The key length of AES-256 is: 128 bits 192 bits 256 bits 512 bits 126 Which attack method tries every possible key? Dictionary attack Chosen-ciphertext attack Brute-force attack Known-key 127 The one-time pad cipher is: Chosen-ciphertext attack Chosen-ciphertext Chosen- | asymmetric |
| 124 Which of these is a stream cipher? DES AES RC4 RSA 125 The key length of AES-256 is: 128 bits 192 bits 256 bits 512 bits 126 Which attack method tries every possible key? Dictionary attack Unbreakable if used Chosen-ciphertext attack An example of block Symmetric and deterministic Obsolete a | |
| 125 The key length of AES-256 is: 128 bits 192 bits 256 bits 512 bits 126 Which attack method tries every possible key? Unbreakable if used correctly Chosen-ciphertext attack An example of block cipher Cipher Obsolete a | |
| 126 Which attack method tries every possible key? Dictionary attack Unbreakable if used Chosen-ciphertext attack An example of block Cipher Chosen-ciphertext attack Symmetric and deterministic Obsolete a | 1 |
| Unbreakable if used An example of block Symmetric and cipher is: Correctly Cipher deterministic Obsolete a | |
| Unbreakable if used An example of block Symmetric and cipher is: Correctly Cipher deterministic Obsolete a | |
| 127 The one-time pad cipher is: correctly cipher deterministic Obsolete a | attack |
| | |
| Hashed Message with Hashed Message Hybrid Message Hidden MA | ıd weak |
| Hashed Message with Hashed Message Hybrid Message Hidden MA | |
| | C Address |
| 128 What does HMAC stand for? Authentication Control Authentication Code Authentication Cipher Cipher | |
| Which property ensures that two different messages | |
| 129 do not have the same hash? Avalanche effect Collision resistance Key expansion Substitutio | 1 |
| Which cipher type relies on permutation of plaintext | |
| 130 characters? Caesar cipher Substitution cipher Transposition cipher Vigenère ci | oher |
| | |
| Stores a full or partial | |
| 131 What does a node in a blockchain network do? Mines coins only copy of the blockchain Encrypts wallets Deletes old | blocks |
| Which of the following is an example of a private | |
| 132 blockchain? Ethereum Bitcoin Ripple Hyperledge | r Fabric |
| Which cryptographic concept does blockchain rely | |
| 133 on for block linkage? One-time pads Stream ciphers Hash functions Symmetric | |
| 134Smart contracts are typically deployed on:BitcoinEthereumDES networksTLS layers | encryption |
| Which type of consensus algorithm is used by Practical By | encryption |
| 135 Bitcoin? Proof of Stake Proof of Authority Proof of Work Tolerance | encryption zantine Fault |

| Srno | Question | Option A | Option B | Option C | Option D |
|------|--|-----------------------------|----------------------------|--------------------------|--------------------------|
| | | | Protect data | | |
| | What is the primary purpose of cryptography in | | confidentiality and | | |
| 136 | cybersecurity? | Increase network speed | integrity | Backup systems | Disable malware |
| | Which of these ciphers was developed during World | | | | |
| 137 | War II? | Vigenère Cipher | Enigma | Caesar Cipher | Playfair Cipher |
| 138 | The Playfair Cipher encrypts text in: | Single letters | Pairs of letters | Binary format | Triple letters |
| | | | | | |
| 139 | Which of the following is not a symmetric cipher? | Blowfish | AES | RSA | DES |
| | | | | Integrity and non- | |
| 140 | A digital signature can provide: | Confidentiality only | Authentication only | repudiation | Key distribution |
| | What is the correct order of digital signature | | | | |
| 141 | creation? | Sign → Hash → Send | Hash → Sign → Send | Encrypt → Hash → Sign | Send → Sign → Hash |
| | Most common output size of the MD5 hash | | | | |
| 142 | algorithm? | 128 bits | 256 bits | 64 bits | 512 bits |
| | | | Control over the | Both plaintext and | Access to the decryption |
| 143 | A known-plaintext attack assumes: | Access to ciphertext only | encryption key | ciphertext are known | algorithm |
| | Which algorithm is considered insecure due to | | | | |
| 144 | collision vulnerabilities? | SHA-256 | AES | MD5 | RSA |
| | | | | | |
| | | Storing encrypted | Backing up private keys | Revoking digital | Generating symmetric |
| 145 | Key escrow is a practice of: | | with a trusted third party | 1 | keys |
| | | | A split in the chain due | | - / - |
| | | | to consensus | A broken cryptographic | A type of hashing |
| 146 | In blockchain, a 'fork' typically refers to: | A loss of encryption keys | | link | algorithm |
| | Which blockchain concept prevents double | , read or end y parent keys | | | |
| 147 | spending? | Hashing | Nonces | Consensus mechanisms | Time-locks |
| | | | Block size affects | | |
| | Which of the following is true about block size in | All blockchains have the | | | It is used only in smart |
| 148 | blockchain? | same block size | capacity | Block size is irrelevant | contracts |
| | • | 2 2 2 2 2 2 2 2 | Verify large sets of data | Generate wallet | |
| 149 | In blockchain, a Merkle tree is used to: | Store private keys | efficiently | addresses | Synchronize clocks |
| | | | | | |
| | | | A blockchain-based | | |
| | | | algorithm that enforces | A type of asymmetric | A password policy for |
| 150 | What is a smart contract? | offline | rules automatically | encryption | blockchain wallets |
| | white is a simult contract: | Jonnie . | i dies automatically | Terror yption | Diockeriani Wanets |